Interference Search

	L #	Search Text	DBs	Time Stamp	Hits
29	L29	generating AND certifying AND asymmetrical AND cryptokey AND trust AND center AND user AND secure AND transmission.CLM.	US-PGPUB	2007/04/10 20:59	0
30	L30	trust AND center AND user AND encryption AND key AND pair AND certified AND signature.CLM.	US-PGPUB	2007/04/10 20:59	54
31	L31	part AND secret AND public AND encryption AND key AND pair AND certified AND signature.CLM.	US-PGPUB	2007/04/10 21:00	227
32	L32	marking AND public AND part AND encryption AND key AND pair AND trust AND center.CLM.	US-PGPUB	2007/04/10 21:00	55
33	L33	unequivocally AND assigning AND one AND encryption AND key AND pair.CLM.	US-PGPUB	2007/04/10 21:01	0
34	L34	new AND certificate AND encrypted AND user.CLM.	US-PGPUB	2007/04/10 21:01	3570
35	L35	checking AND correctness AND bilateral AND communication AND verifying AND signature.CLM.	US-PGPUB	2007/04/10 21:02	1
36	L36	checking AND genuineness AND validity AND new AND certificate AND trust AND center.CLM.	US-PGPUB	2007/04/10 21:02	1

	Comments
29	
30	
31	
32	
33	
34	
35	
36	

Web Results **1 - 1** of **1** for **trust center, certificate, encryption, signature key pair, bilateral communication**

Tip: Try removing quotes from your search to get more results.

CIPO - Canadian Patent Database - Claims - 2283178
(b) next, the user generates his own additional **encryption key pair** with a ... no **communication** with the **trust centre**, during each **bilateral communication** ...
patents1.ic.gc.ca/claims?patent_number=2283178&language= - 11k -
Cached - Similar pages

Terms used
asymmetrical cryptographic keys trust center certificate encryption signature key pair bilateral communica

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Gu

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance sca

1 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index term

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prol practical data processing systems in the 1980s. As we have come to rely on these systems to p and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communic systems from unauthorized disclosure ...

2 Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

3 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue :

Publisher: ACM Press

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index term

We study protocols for strong authentication and key exchange in asymmetric scenarios where authentication server possesses ~a pair of private and public keys while the client has only a w human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocol formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwo

public-key protocols

4 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4
Publisher: ACM Press
Full text available: pdf(3.37 MB) Additional Information: full citation, abstract, references, citings, index term

We describe a theory of authentication and a system that implements it. Our theory is based on notion of principal and a "speaks for" relation between principals. A simple principal either has a or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribut loading programs, path name, principal, role, secure channel, speaks for, trusted computing ba

5 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration

Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(107.24 KB) Additional Information: full citation, abstract, references, index terms

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the U architecture carry the heritage of the GSM's philosophy regarding the user/network authenticati the data ciphe ...

Keywords: PKIs, PLMNs, asymmetric cryptography

6 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth AC symposium on Operating systems principles SOSP '91**, Volume 25 Issue 5
Publisher: ACM Press
Full text available: pdf(2.33 MB) Additional Information: full citation, abstract, references, citings, index term

We describe a theory of authentication and a system that implements it. Our theory is based on notion of principal and a "speaks for" relation between principals. A simple principal either has a or is a communication channel; a compound principal can express an adopted role or delegatior authority. The theory explains how to reason about a principal's authority by deducing the othei principals that it can speak for; authenticating a channel is one important application. We use th

7 Just fast keying: Key agreement in a hostile internet

William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, (Reingold
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2
Publisher: ACM Press
Full text available: pdf(324.39 KB) Additional Information: full citation, abstract, references, citings, index term

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property also has a number of novel engineering parameters that permit a variety of tradeoffs, most noti ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

8 Secret key distribution protocol using public key cryptography

Amit Parnerkar, Dennis Guster, Jayantha Herath

October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

Publisher: Consortium for Computing Sciences in Colleges

Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorith key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret transferred with the help of public key cryptography. The authentication process is accomplishe using the message digest algorithm MD5. This protocol uses mutual authentication in which, bo participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

9 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for con communications SIGCOMM '04**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, citings, index term

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of tl underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has bec priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particula study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

10 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler

September 2002 **Wireless Networks**, Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index term

Wireless sensor networks will be widely deployed in the near future. While much research has f on making these networks feasible and useful, security has received little attention. We present of security protocols optimized for sensor networks: SPINS. SPINS has two secure building bloc SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evide data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc ne secrecy and confidentiality, secure communication protocols, sensor networks

11 Security: Fast authenticated key establishment protocols for self-organizing sensor networ

Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, Jinyun Zhang
September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications WSNA '03**
Publisher: ACM Press
Full text available: pdf(303.05 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we consider efficient authenticated key establishment protocols between a sensor security manager in a self-organizing sensor network. We propose a hybrid authenticated key establishment scheme, which exploits the difference in capabilities between security managers a sensors, and put the cryptographic burden where the resources are less constrained. The hybric scheme reduces the high cost public-key operations at the sensor side and replaces them with e symmetric- ...

Keywords: elliptic curve cryptography, key establishment, security, sensor network

12 Crypto-based identifiers (CBIDs): Concepts and applications
Gabriel Montenegro, Claude Castelluccia
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issu
Publisher: ACM Press
Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, citings, index term

This paper addresses the identifier ownership problem. It does so by using characteristics of Sta Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, oppo encryption

13 Verifiable encryption of digital signatures and applications
Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issu
Publisher: ACM Press
Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We ma of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protoc if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fa exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowle public-key cryptography

14 Access management for distributed systems: Peer-to-peer access control architecture usir trusted computing technology
Ravi Sandhu, Xinwen Zhang
June 2005 **Proceedings of the tenth ACM symposium on Access control models and techn SACMAT '05**
Publisher: ACM Press
Full text available: pdf(215.48 KB) Additional Information: full citation, abstract, references, citings, index term

It has been recognized for some time that software alone does not provide an adequate founda building a high-assurance trusted platform. The emergence of industry-standard trusted compu

technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for sec peer-to-peer environments. In this paper we propose a trusted computing architecture to enfor

Keywords: access control, policy enforcement, security architecture, trusted computing

15 A modular approach to the design and analysis of authentication and key exchange protoc (extended abstract)

Mihir Bellare, Ran Canetti, Hugo Krawczyk

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing S '98**

Publisher: ACM Press

Full text available: pdf(1.61 MB) Additional Information: full citation, references, citings, index terms

16 Analyzing security protocols with secrecy types and logic programs

Martín Abadi, Bruno Blanchet

January 2005 **Journal of the ACM (JACM)**, Volume 52 Issue 1

Publisher: ACM Press

Full text available: pdf(438.64 KB) Additional Information: full citation, abstract, references, citings, index term

We study and further develop two language-based techniques for analyzing security protocols. (based on a typed process calculus; the other, on untyped logic programs. Both focus on secrecy properties. We contribute to these two techniques, in particular by extending the former with a generic treatment of many cryptographic operations. We also establish an equivalence between techniques.

Keywords: Cryptographic protocols, logic programming, process calculi, secrecy properties, ty

17 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings

18 Cryptographic tools: ID-based encryption for complex hierarchies with applications to forwa security and broadcast encryption

Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya

October 2004 **Proceedings of the 11th ACM conference on Computer and communications s CCS '04**

Publisher: ACM Press

Full text available: pdf(220.00 KB) Additional Information: full citation, abstract, references, index terms

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys w time. Forward security has several unique requirements in hierarchical identity-based encryptio scheme: (1) users join dynamically; (2) encryption is joining-time-oblivious; (3) users evolve se keys autonomously.

We present a scalable forward-secure HIBE (fs-HIBE) scheme satisfying the above properties. W show how our fs-HIBE scheme can be used to construct a forward-secure ...

Keywords: ID-Based encryption, broadcast encryption, forward security

19 Security protocols: Certified mailing lists

Himanshu Khurana, Hyung-Seok Hahm
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(431.56 KB) Additional Information: full citation, abstract, references, index terms

Email List Services (or simply, *mailing lists*) are becoming increasingly common for collaborative computing. In order to enable their use for official purposes with increased effectiveness and se services typically provided by postal mail (e.g. fair delivery) need to be provided in mailing lists paper we propose a novel Certified Mailing-list Protocol (CMLP) that provides fair delivery, confidentiality, non-repudiation of origin and receipt, and authentication and integrit ...

Keywords: certified delivery, mailing lists

20 The KryptoKnight family of light-weight protocols for authentication and key distribution
Ray Bird, Inder Gopal, Amir Herzberg, Phil Janson, Shay Kutten, Refik Molva, Moti Yung
February 1995 **IEEE/ACM Transactions on Networking (TON)**, Volume 3 Issue 1
Publisher: IEEE Press
Full text available: pdf(1.64 MB) Additional Information: full citation, references, citings, index terms, review

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Results for "((asymmetrical cryptographic keys, trust center, certificate, encryption, signature key pair, bilate..." e-mail

Your search matched **3095** of **1540244** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

view selected items Select All Deselect All View: **1-25** | 26-5

1. **Configuring enterprise public key infrastructures to permit integrated dep signature, encryption and access control systems**
Williams, C.K.;
Military Communications Conference, 2005. MILCOM 2005. IEEE
17-20 Oct. 2005 Page(s):2172 - 2175 Vol. 4
Digital Object Identifier 10.1109/MILCOM.2005.1605991
AbstractPlus | Full Text: PDF(4104 KB) IEEE CNF
Rights and Permissions

2. **Key management for heterogeneous ad hoc wireless networks**
Seung Yi; Kravets, R.;
Network Protocols, 2002. Proceedings. 10th IEEE International Conference on
12-15 Nov. 2002 Page(s):202 - 203
AbstractPlus | Full Text: PDF(226 KB) IEEE CNF
Rights and Permissions

3. **PKI and digital certification infrastructure**
Hunt, R.;
Networks, 2001. Proceedings. Ninth IEEE International Conference on
10-12 Oct. 2001 Page(s):234 - 239
Digital Object Identifier 10.1109/ICON.2001.962346
AbstractPlus | Full Text: PDF(564 KB) IEEE CNF
Rights and Permissions

4. **Applications in health care using public-key certificates and attribute cer**
Wohlmacher, P.; Pharow, P.;
Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference
11-15 Dec. 2000 Page(s):128 - 137
Digital Object Identifier 10.1109/ACSAC.2000.898866
AbstractPlus | Full Text: PDF(864 KB) IEEE CNF
Rights and Permissions

5. **Protocol independence through disjoint encryption**
Guttman, J.D.; Thayer, F.J.F.;
Computer Security Foundations Workshop, 2000. CSFW-13. Proceedings. 13t
3-5 July 2000 Page(s):24 - 34
Digital Object Identifier 10.1109/CSFW.2000.856923

AbstractPlus | Full Text: PDF(344 KB) IEEE CNF
Rights and Permissions

6. **Increasing user privacy in online transactions with X.509 v3 certificate pr and smartcards**
Rexha, B.;
E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Confe
19-22 July 2005 Page(s):293 - 300
Digital Object Identifier 10.1109/ICECT.2005.54
AbstractPlus | Full Text: PDF(184 KB) IEEE CNF
Rights and Permissions

7. **Biometrics electronic purse**
Wahab, A.; Tan, E.C.; Heng, S.M.;
TENCON 99. Proceedings of the IEEE Region 10 Conference
Volume 2, 15-17 Sept. 1999 Page(s):958 - 961 vol.2
Digital Object Identifier 10.1109/TENCON.1999.818579
AbstractPlus | Full Text: PDF(344 KB) IEEE CNF
Rights and Permissions

8. **Design of a key agile cryptographic system for OC-12c rate ATM**
Stevenson, D.; Hillery, N.; Byrd, G.; Fengmin Gong; Winkelstein, D.;
Network and Distributed System Security, 1995., Proceedings of the Symposiu
16-17 Feb. 1995 Page(s):17 - 30
Digital Object Identifier 10.1109/NDSS.1995.390648
AbstractPlus | Full Text: PDF(1020 KB) IEEE CNF
Rights and Permissions

9. **Bulk encryption crypto-processor for smart cards: design and implement**
Sklavos, N.; Selimis, G.; Koufopavlou, O.;
Electronics, Circuits and Systems, 2004. ICECS 2004. Proceedings of the 200
International Conference on
13-15 Dec. 2004 Page(s):579 - 582
Digital Object Identifier 10.1109/ICECS.2004.1399747
AbstractPlus | Full Text: PDF(524 KB) IEEE CNF
Rights and Permissions

10. **A generic secure Internet-based facility to support multiple registries usi encryption technology and client certificates**
Dassen, W.R.M.; Gommer, E.D.; Bonnemayer, C.C.W.; Spruijt, H.J.; Dijk, W.A
Computers in Cardiology, 2002
22-25 Sept. 2002 Page(s):273 - 276
AbstractPlus | Full Text: PDF(498 KB) IEEE CNF
Rights and Permissions

11. **A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amo**
Mohammad Zakir Hossain Sarker; Md. Shafiul Parvez;
9th International Multitopic Conference, IEEE INMIC 2005
Dec. 2005 Page(s):1 - 6
Digital Object Identifier 10.1109/INMIC.2005.334435
AbstractPlus | Full Text: PDF(92 KB) IEEE CNF
Rights and Permissions

12. **Explicit Exclusive Set Systems with Applications to Broadcast Encryptio**
Gentry, C.; Ramzan, Z.; Woodruff, D.P.;
Foundations of Computer Science, 2006. FOCS '05. 47th Annual IEEE Sympo
Oct. 2006 Page(s):27 - 38
Digital Object Identifier 10.1109/FOCS.2006.27

AbstractPlus | Full Text: PDF(208 KB) IEEE CNF
Rights and Permissions

13. **CONSEPP: CONvenient and secure electronic payment protocol based o**
Levi, A.; Koc, C.K.;
Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings
10-14 Dec. 2001 Page(s):286 - 295
AbstractPlus | Full Text: PDF(208 KB) IEEE CNF
Rights and Permissions

14. **E-DHCP: extended dynamic host configuration protocol**
Demerjian, J.; Serhrouchni, A.;
Information and Communication Technologies: From Theory to Applications, 2
Proceedings. 2004 International Conference on
19-23 Apr 2004 Page(s):667 - 668
Digital Object Identifier 10.1109/ICTTA.2004.1307942
AbstractPlus | Full Text: PDF(297 KB) IEEE CNF
Rights and Permissions

15. **Hierarchical key management for mobile ad-hoc networks**
Budakoglu, C.; Gulliver, T.A.;
Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th
Volume 4, 26-29 Sept. 2004 Page(s):2735 - 2738 Vol. 4
Digital Object Identifier 10.1109/VETECF.2004.1400555
AbstractPlus | Full Text: PDF(490 KB) IEEE CNF
Rights and Permissions

16. **A protocol for establishing secure communication channels in a large ne**
Harn, L.; Huang, D.;
Knowledge and Data Engineering, IEEE Transactions on
Volume 6, Issue 1, Feb. 1994 Page(s):188 - 191
Digital Object Identifier 10.1109/69.273037
AbstractPlus | Full Text: PDF(320 KB) IEEE JNL
Rights and Permissions

17. **Verifying the SET registration protocols**
Bella, G.; Massacci, F.; Paulson, L.C.;
Selected Areas in Communications, IEEE Journal on
Volume 21, Issue 1, Jan. 2003 Page(s):77 - 87
Digital Object Identifier 10.1109/JSAC.2002.806133
AbstractPlus | References | Full Text: PDF(641 KB) IEEE JNL
Rights and Permissions

18. **A soft dynamic service specific trust management and authentication scl adhoc networks**
Bhattacharyya, M.; Nandi, S.; Saha, S.;
Wireless and Optical Communications Networks, 2006 IFIP International Confe
11-13 April 2006 Page(s):5 pp.
Digital Object Identifier 10.1109/WOCN.2006.1666569
AbstractPlus | Full Text: PDF(1008 KB) IEEE CNF
Rights and Permissions

19. **Secure email-based peer to peer information retrieval**
Chengye Lu; Geva, S.;
Cyberworlds, 2005. International Conference on
23-25 Nov. 2005 Page(s):8 pp.
Digital Object Identifier 10.1109/CW.2005.80
AbstractPlus | Full Text: PDF(248 KB) IEEE CNF
Rights and Permissions

20. **Internet security**
Issa, N.;
Information and Communication Technologies: From Theory to Applications, 2
Proceedings. 2004 International Conference on
19-23 April 2004 Page(s):623
Digital Object Identifier 10.1109/ICTTA.2004.1307918
AbstractPlus | Full Text: PDF(205 KB) IEEE CNF
Rights and Permissions

21. **WEDDS: the WITS encrypted data delivery system**
Norris, J.S.; Backes, P.G.;
Aerospace Conference Proceedings, 2000 IEEE
Volume 2, 18-25 March 2000 Page(s):359 - 366 vol.2
Digital Object Identifier 10.1109/AERO.2000.878243
AbstractPlus | Full Text: PDF(688 KB) IEEE CNF
Rights and Permissions

22. **Access control in an open distributed environment**
Hayton, R.J.; Bacon, J.M.; Moody, K.;
Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on
3-6 May 1998 Page(s):3 - 14
Digital Object Identifier 10.1109/SECPRI.1998.674819
AbstractPlus | Full Text: PDF(204 KB) IEEE CNF
Rights and Permissions

23. **Some Remarks on the Certificates Registration of the Electronic Comme**
Brlek, S.; Hamadou, S.; Mullins, J.;
Telecommunications, 2006. AICT-ICIW '06. International Conference on Intern
Applications and Services/Advanced International Conference on
19-25 Feb. 2006 Page(s):119 - 119
Digital Object Identifier 10.1109/AICT-ICIW.2006.176
AbstractPlus | Full Text: PDF(232 KB) IEEE CNF
Rights and Permissions

24. **Implementing a fully distributed certificate authority in an OLSR MANET**
Dhillon, D.; Randhawa, T.S.; Wang, M.; Lamont, L.;
Wireless Communications and Networking Conference, 2004. WCNC. 2004 IE
Volume 2, 21-25 March 2004 Page(s):682 - 688 Vol.2
AbstractPlus | Full Text: PDF(460 KB) IEEE CNF
Rights and Permissions

25. **Quantitative analysis of security protocols in wireless networks**
Best, P.; Kamesh Namuduri; Pendse, R.;
Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics
18-20 June 2003 Page(s):290 - 291
AbstractPlus | Full Text: PDF(364 KB) IEEE CNF
Rights and Permissions

View: **1-25** | 26-5

	L #	Search Text	DBs	Time Stamp	Hits
1	L1	"generat$3" near "asymmetrical crytokey" near "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0
2	L2	"generat$3" same "asymmetrical crytokey" near "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:50	0
3	L3	"generat$3" same "asymmetrical crytokey" same "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:50	0

	L #	Search Text	DBs	Time Stamp	Hits
4	L4	(generat$3) same "asymmetrical crytokey" same "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0
5	L5	(generat$3) and "asymmetrical crytokey" and "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:50	0
6	L6	"asymmetrical crytokey" and "user" and "trust center"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0

	L #	Search Text	DBs	Time Stamp	Hits
7	L7	"asymmetrical cryptokey" and "user" and "trust center"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0
8	L8	"generat$3" near "asymmetrical cryptokey" near "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0
9	L9	(generat$3) same "asymmetrical cryptokey" same "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:51	0

	L #	Search Text	DBs	Time Stamp	Hits
10	L10	"trust center" and "user" and "certified signature" and "key pair"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:52	1
11	L11	"encryption key pair" and "public" and "secret"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:52	203
12	L12	"trust center" and "unequivocally assignment" and "signature key pair"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:53	0

	L #	Search Text	DBs	Time Stamp	Hits
13	L13	(encrypt$3) same (certificate) same (encryption key pair)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:53	7850
14	L14	L11 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:53	113
15	L15	L14 and L10	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:54	0

	L #	Search Text	DBs	Time Stamp	Hits
16	L16	L14 and "bilateral communication"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:54	0
17	L17	L14 and "no communication"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:54	3
18	L18	L17 and "genuineness" and "validity"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:55	0

	L #	Search Text	DBs	Time Stamp	Hits
19	L19	713/156.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:55	823
20	L20	713/156.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:55	17
21	L21	713/158.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:55	1

	L #	Search Text	DBs	Time Stamp	Hits
22	L22	380/277.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:56	18
23	L23	380/278.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:56	17
24	L24	deutsche.asn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:56	9340

	L #	Search Text	DBs	Time Stamp	Hits
25	L25	mertes.in. and paul.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:56	20
26	L26	mettken.in. and werner.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:56	6
27	L27	L25 and L26	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:57	1

	L #	Search Text	DBs	Time Stamp	Hits
28	L28	L27 and L24	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/04/10 20:57	1